

What is claimed is:

1. An apparatus connected between a network access unit and a network to be protected, for protecting legitimate traffic from DoS and DDoS attacks, comprising:
 - 5 a high-priority queue;
 - a low-priority queue;
 - a queue information table having specific STT service queue information of a specific packet;
 - 10 a queue coordinator for updating the queue information table based on a load of a provided STT and a load of the high-priority queue;
 - a packet classifier for receiving a packet from the network access unit, investigating an STT service queue of the received packet from the queue information table,
15 selectively transferring the received packet to the high-priority queue or the low-priority queue in accordance with an investigation result and providing information on the received packet to the queue coordinator; and
 - 20 a buffer for buffering outputs of the high-priority queue and the low-priority queue and providing buffered outputs to the network to be protected.
2. The apparatus of claim 1, wherein the network to be
25 protected comprises a server.
3. The apparatus of claim 1, wherein the information on the received packet includes a packet size, a packet arrival time and an index of the queue information table for
30 representing STT information of the packet.
4. The apparatus of claim 1, wherein the queue information table has fields including an STT ID, a service queue, an average load, a recent load calculation time and a
35 total packet size.

5. The apparatus of claim 1, wherein a maximum load of the high-priority queue and the low-priority queue is set to be a maximum allowable load of the network to be protected.

5 6. The apparatus of claim 5, wherein the network to be protected comprises a server.

7. A method for protecting legitimate traffic from DoS and DDoS attacks in an apparatus therefor, wherein the
10 apparatus is connected between a network access unit and a network to be protected and includes a queue information table having specific STT service queue information of a specific packet, a queue coordinator for updating the queue information table based on a load of a provided STT and a
15 load of a high-priority queue and a packet classifier for receiving a packet from the network access unit, investigating an STT service queue of a received packet from the queue information table, selectively transferring the received packet to the high-priority queue or the low-
20 priority queue in accordance with an investigation result and providing information on the received packet to the queue coordinator, the method comprising the steps of:

(a) obtaining an STT ID based on a source IP address of the packet received from the network access unit;

25 (b) investigating a service queue corresponding to the searched STT ID from the queue information table and checking whether the service queue is the high-priority queue or the low-priority queue;

(c) transferring the received packet to the high-
30 priority queue if the service queue is the high-priority queue in the step (b);

(d) transferring the received packet to the low-priority queue if the service queue is the low-priority queue in the step (b); and

35 (e) transferring the received packet information to the queue coordinator.

8. The method of claim 7, wherein the network to be protected comprises a server.

5 9. The method of claim 7, wherein the queue coordinator comprises the steps of:

(a') calculating an average load of an STT corresponding to the packet information transferred from the packet classifier;

10 (b') resetting an STT service queue based on the calculated average load of the STT;

(c') calculating an average load of the high-priority queue;

15 (d') resetting a certain STT service queue based on the calculated average load of the high-priority queue; and

(e') storing the reset STT information in the queue information table.

20 10. The method of claim 9, wherein the modified STT information refers to a modified average load and service queue.

11. The method of claim 9, wherein the step (a') further includes the steps of:

25 (a'1) calculating a total packet size based on the packet information transferred from the packet classifier;

(a'2) checking whether it is time to recalculate an average load;

30 (a'3) calculating a new average load by using a previous average load and a current average load based on the total packet size if it is time to recalculate the average load in the step (a'2); and

35 (a'4) performing an STT service queue determination algorithm based on the load of the STT if it is not time to recalculate the average load or subsequent to executing the step (a'3).

12. The method of claim 11, wherein the packet information includes a packet size, a packet arrival time, a queue information table index and a corresponding STT.

5

13. The method of claim 9, wherein the step (b') further includes the steps of:

(b'1) setting an STT service queue of a received packet to be a the low-priority queue if an STT load of the received packet is greater than an allowable load when the high-priority queue is in a congested state;

(b'2) randomly choosing one STT using a low-priority queue from the queue information table if the service queue of the STT corresponding to the received packet is a high-priority queue;

(b'3) setting an STT service queue of a low load to be a high-priority queue and an STT service queue of a high load to be a low-priority queue if an average load of an STT corresponding to the received packet is greater than that of the randomly chosen STT;

(b'4) randomly choosing one STT using a high-priority queue from the queue information table if the service queue of the STT corresponding to the received packet is a low-priority queue; and

(b'5) setting an STT service queue of a low load to be a high-priority queue and the STT service queue of a high load to be a low-priority queue if an average load of an STT corresponding to the received packet is smaller than that of the randomly chosen STT.

30

14. The method of claim 9, wherein the step (c') further includes the steps of:

(c'1) determining an STT service queue based on a load of an STT;

(c'2) calculating a total packet size served through a high-priority queue if the service queue used by the

35

received packet is a high-priority queue;

(c'3) calculating an average load of a high-priority queue if it is time to recalculate a load;

(c'4) resetting a certain STT service queue based on
5 the load of the high-priority queue; and

(c'5) storing modified STT information in the queue information table.

15 15. The method of claim 9, wherein the step (d') includes the steps of:

(d'1) calculating an average load of a high-priority queue;

(d'2) randomly choosing one STT using a high-priority queue and setting a queue of the STT to low-priority if the
15 load of the high-priority queue is in a congested state;

(d'3) randomly choosing one STT using a low-priority queue and setting a queue of the STT to high-priority if the load of the high-priority queue is in an idle state; and

(d'4) storing modified STT information in the queue
20 information table if the load of the high-priority queue is in a stable state or the steps of (d'2) and (d'3) are performed.